Présentation de solution

Halte à l'exfiltration de données

Protégez votre ressources inestimables.

Le **Rapport de McAfee® Labs sur le paysage des menaces — Août 2015** se penche sur une étape majeure du processus de vol de données : leur exfiltration. Elle consiste pour le cyberescroc à copier ou à déplacer les données qu'il convoite, du réseau de leur propriétaire vers un autre que lui-même contrôle.

Au cours des dix dernières années, le nombre de compromissions de données et de leurs victimes a augmenté de façon phénoménale. Il ne s'agit plus de collecter des numéros de cartes de crédit et de débit, mais de dérober pratiquement toutes les informations que nous mettons en ligne : noms, dates de naissance, adresses, numéros de téléphone, données médicales, identifiants de compte, et bien d'autres encore.

Les particuliers ne sont pas les seules cibles. Le cyberespionnage par des États, des organisations criminelles et des cyberactivistes met constamment en péril les données sensibles des citoyens, des organismes publics et des entreprises.

Auteurs d'attaques et motivations

Un auteur d'attaques, ou attaquant, est un groupe ou un individu dont l'intention est d'obtenir un accès non autorisé à des réseaux et systèmes informatiques. La communauté de la sécurité informatique met en évidence trois grandes catégories d'auteurs d'attaques : les États, les organisations criminelles et les cyberactivistes. Le tableau ci-dessous propose un aperçu de leurs motivations et des types de données qu'ils convoitent généralement en raison de leur valeur.

	États	Crime organisé	Cyberactivistes
Motivations générales	Espionnage Influence	Motivations financières	Atteinte à la réputation Médias sociaux
Exemples de types de données	Code source E-mails Documents internes Activité militaire Informations d'identification personnelle de fonctionnaires	Informations bancaires Données de cartes de crédit Informations d'identification personnelle (numéros de sécurité sociale, données médicales, etc.)	E-mails Informations sur le personnel Tous types de données internes sensibles
Volume des données convoitées	Faible à élevé	Élevé	Faible à élevé
Niveau de sophistication des techniques d'exfiltration	Élevé	Moyen à faible	Moyen à faible
Emplacement sur le réseau	Inconnu/données souvent disséminées	Connu	À la fois connu et inconnu/ données souvent disséminées

intel Security

Données cibles

Dès qu'un attaquant compromet un système du réseau, il commence à explorer d'autres systèmes pour identifier ceux susceptibles de contenir les données qui l'intéressent. Comme un réseau complexe héberge de nombreux types de données, un auteur d'attaques ne disposant pas de connaissances privilégiées mettra du temps à y parvenir, ce qui augmente la probabilité qu'il soit détecté. D'où la nécessité de concevoir des attaques aussi furtives et persistantes que possible.

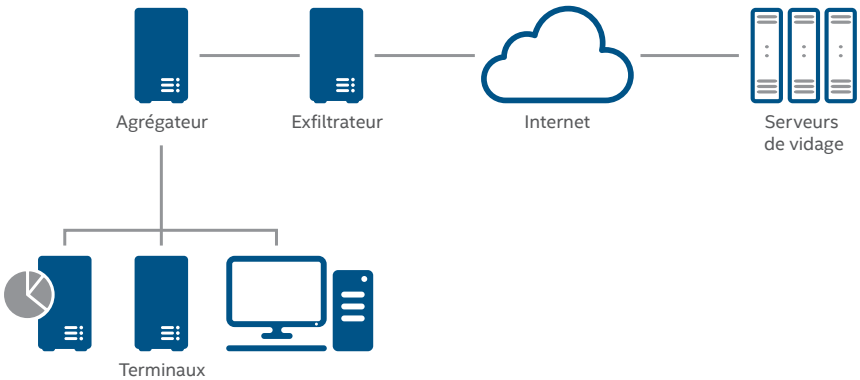
Selon leur catégorie, les auteurs d'attaques s'intéressent à des cibles et à des types de données différents :

Cibles de données	Types de données	Auteurs d'attaques potentiels
Systèmes de base de données	Informations médicales protégées, informations d'identification personnelle, cartes de crédit, comptes bancaires et comptes d'utilisateur	Organisations criminelles, cyberactivistes
Référentiels de code source	Code source, informations d'identification, clés	États, cyberactivistes
Systèmes spécialisés	Variables	Tous, selon le type de terminal
Partages de fichiers et systèmes similaires	Code source, plans, communications	États, cyberactivistes
E-mails et communications	Plans, communications	États, cyberactivistes

Exfiltration des données

Dès qu'un auteur d'attaques a localisé et mis la main sur les données qu'il recherche, le plus dur reste à faire : les exfiltrer. Il utilise l'environnement de l'hôte en tant qu'intermédiaire entre son propre réseau et celui de la victime. Cette infrastructure relais peut être complexe ou simple, selon que les données cibles sont plus ou moins segmentées et enfouies dans les profondeurs du réseau. Les types de systèmes suivants peuvent être utilisés dans une infrastructure relais :

- **Terminaux —** Une ou plusieurs cibles de données sur le même segment ou un segment routable vers l'agrégateur.
- **Agrégateur —** Sert de point de collecte pour les données des terminaux cibles et télécharge les données vers l'exfiltrateur. L'agrégateur peut avoir, ou non, accès à Internet. Dans le cadre de campagnes sophistiquées, plusieurs agrégateurs peuvent transférer les données vers plusieurs exfiltrateurs pour dissimuler le chemin de sortie des données.
- **Exfiltrateur —** Récupère les données d'un agrégateur et facilite leur transfert vers le serveur de vidage de l'attaquant. Soit l'exfiltrateur se contente de transférer les données, soit il les conserve jusqu'à ce que l'attaquant les récupère.



Architecture d'exfiltration des données classique

Que sa tâche soit aisée ou compliquée, l'objectif de l'attaquant est de transférer les données ciblées vers un serveur situé hors du réseau de la victime. Le serveur de vidage est le premier emplacement en dehors du contrôle de la victime dans lequel sont hébergées les données volées et auquel l'attaquant peut facilement accéder. Divers systèmes peuvent jouer le rôle de serveurs de vidage :

- **Systèmes compromis —** Systèmes compromis par l'attaquant lors d'une autre campagne. Ils peuvent prendre diverses formes dont, entre autres, des blogs WordPress personnels ou des serveurs appartenant à des sociétés dotées de contrôles de sécurité insuffisants.
- **Systèmes hébergés dans des pays particuliers —** Les pays possédant une législation stricte en matière de confidentialité sont intéressants pour les attaquants car les systèmes hébergés au sein de leurs frontières jouissent d'un certain degré de protection et d'impunité.
- **Systèmes hébergés temporairement —** Systèmes éphémères hébergés dans le cloud via des fournisseurs tels qu'Amazon Web Services, Digital Ocean ou Microsoft Azure.
- **Services cloud de partage de fichiers —** Sites de partage de fichiers en ligne à accès libre, par exemple DropBox, Box.com ou Pastebin.
- **Services hébergés dans le cloud —** Autres services Internet tels que Twitter et Facebook permettant à leurs utilisateurs de publier des données.

Transports de données

Les transports de données sont des protocoles et des méthodes utilisés par les cyberescrocs pour copier les données d'un emplacement ou d'un système à un autre. Ces derniers peuvent être soit tous les deux internes (terminal vers agrégateur), soit l'un interne et l'autre externe (exfiltrateur vers serveur de vidage). Le tableau ci-dessous récapitule les protocoles de transport les plus fréquemment utilisés :

Transport	Description	Interne	Externe
HTTP/HTTPS	La prévalence de HTTP dans les communications réseau en fait le protocole idéal pour dissimuler des données exfiltrées dans d'autres flux de trafic. Souvent utilisée pour l'exfiltration des données, cette méthode incorpore les commandes dans les en-têtes HTTP et les méthodes GET/POST/PUT.		■
FTP	Généralement disponible sur les serveurs d'entreprise, FTP est un protocole de transport très simple à utiliser avec des commandes système natives.	■	■
USB	Les périphériques de stockage USB sont souvent utilisés pour l'exfiltration dans des réseaux isolés. Certains logiciels malveillants recherchent une clé USB affectée d'un marqueur spécifique, puis copient les données à exfiltrer vers un secteur masqué de la clé. Lorsque la clé est insérée dans un autre système infecté connecté au réseau, le processus d'exfiltration démarre. Les clés USB peuvent être également utilisées par des utilisateurs internes pour copier facilement d'importants volumes de données et les sortir physiquement de l'entreprise.	■	■
DNS	Des enregistrements DNS spécifiques, notamment des enregistrements TXT ou A et CNAME peuvent, dans une certaine mesure, stocker des données. Grâce au contrôle d'un domaine et d'un serveur de noms, un attaquant peut transférer des petits volumes de données en effectuant des recherches spécifiques sur le système chargé de l'exfiltration.		■
Tor	L'utilisation du réseau Tor tend à se généraliser. Il permet aux attaquants de publier des données exfiltrées sur des serveurs difficiles à identifier. Toutefois, le trafic Tor sur les réseaux d'entreprise est rarement légitime et peut donc être facilement détecté et bloqué.		■
SMTP/E-mail	Il est possible d'utiliser les serveurs SMTP appartenant ou non à la société pour envoyer des données à l'extérieur de l'entreprise sous la forme de pièces jointes ou dans le corps des messages e-mail.		■
SMB	SMB est un protocole très courant dans les environnements Microsoft Windows et est parfois déjà activé sur certains systèmes.	■	
RDP	RDP prend en charge différentes activités, dont le copier-coller et le partage des fichiers. Dans certains cas, les systèmes autorisant RDP peuvent être exposés à Internet.	■	■
Transports personnalisés	Les transports personnalisés sont parfois utilisés dans les communications du serveur de contrôle et les logiciels malveillants évolués. Pour être robuste, un transport nécessite d'importants efforts de développement et sa singularité facilite sa détection sur le réseau, ce qui fait pencher la balance en faveur d'un protocole de transport établi.	■	■

Manipulation de données

Les attaquants prendront toutes les mesures nécessaires pour que leurs cibles ne s'aperçoivent pas qu'ils manipulent et exfiltrent des données sensibles. La manipulation des données avant leur transfert peut contribuer à éviter la détection, à diminuer le temps de transfert et à augmenter les délais d'identification. Voici quelques-unes des techniques principalement utilisées lors de cette phase :

Technique	Description
Compression	La compression au format .ZIP standard offre non seulement un certain degré de dissimulation, mais elle accélère également les transferts de fichiers.
Segmentation	Le fractionnement des données en petits blocs avant l'envoi permet de mêler le transfert aux activités réseau normales.
Codage et obscurcissement	La forme la plus courante de manipulation des données est l'algorithme de codage ou d'obscurcissement. À l'aide de techniques simples telles que l'exécution d'une opération XOR avec une clé statique, le codage en Base64 ou la conversion de chaque caractère au format hexadécimal, il est possible de manipuler juste assez les données pour éviter toute détection.
Chiffrement	Paradoxalement, le chiffrement n'est pas toujours utilisé au cours de l'exfiltration. Ce peut être dû au fait qu'il ralentit les performances ou qu'il ne se justifie pas vraiment. S'il est utilisé, il s'agira vraisemblablement d'un chiffrement RC4 ou AES.

Comment Intel Security peut vous aider à vous protéger contre l'exfiltration de données

McAfee DLP Discover

Pour sécuriser efficacement vos données, la première étape consiste à comprendre où elles se trouvent et quelle est leur nature. **McAfee DLP Discover** simplifie cette étape grâce à plusieurs fonctionnalités de façon à vous protéger contre l'exfiltration de données :

- **Identification et contrôle des données sensibles —** McAfee DLP Discover analyse de façon automatisée l'ensemble des ressources disponibles, puis inventorie et indexe la totalité du contenu : vous pouvez ainsi mieux identifier vos données sensibles et leur emplacement. La solution permet d'exécuter des requêtes et d'explorer les informations résultantes pour déterminer comment elles sont utilisées, qui en est le propriétaire, où elles sont stockées et les destinations de leurs transferts.
- **Évaluation des infractions et application de mesures correctives —** La solution détecte les infractions aux stratégies relatives au contenu, enregistre et génère des signatures, puis envoie des notifications d'alerte pour que la protection des données sensibles soit renforcée. L'intégration avec la gestion des incidents et la gestion des cas limite la prolifération des informations sensibles.
- **Définition aisée de stratégies de protection —** La création et la gestion des stratégies, de même que la génération de rapports, s'effectuent de manière à la fois intuitive et centralisée. Vous bénéficiez ainsi d'un contrôle accru sur votre stratégie globale de protection des informations.

McAfee DLP Monitor

McAfee DLP Monitor collecte et suit les données en mouvement sur l'ensemble du réseau et génère les rapports correspondants. Il vous permet de détecter facilement les menaces inconnues visant les données et de prendre les mesures requises pour les protéger, afin d'éviter que votre entreprise ait à pâtir d'une compromission massive.

- **Examen du trafic réseau —** La technologie ultraperformante de balayage et d'analyse des données de McAfee DLP Monitor effectue un examen approfondi du trafic réseau.
- **Identification rapide des données —** La fonction de découverte en temps réel permet de déterminer rapidement l'usage qui est fait des données, les personnes qui les utilisent et leur destination, de sorte que vous disposez d'informations permettant de prendre

les mesures qui s'imposent. McAfee DLP Monitor est à même de détecter rapidement plus de 300 types de contenu transitant par n'importe quel port ou employant n'importe quel protocole, les empêchant ainsi de passer inaperçus aux yeux de votre entreprise.

- **Exécution d'investigations numériques détaillées —** Des investigations numériques permettent de mettre en corrélation les événements, passés et présents, associés à un risque, de détecter les tendances des risques et d'identifier les menaces. Grâce à McAfee DLP Monitor, vous appréhendez rapidement la situation et vous pouvez élaborer des règles et stratégies pour y remédier.

McAfee DLP Prevent

McAfee DLP Prevent vous protège contre les fuites de données en s'assurant que celles-ci ne quittent le réseau que moyennant autorisation — que ce soit par le biais de la messagerie électronique, de la messagerie web, de la messagerie instantanée, de wikis, de blogs, de portails, de sites HTTP/HTTPS ou de transferts FTP. Toute la différence entre garder vos précieuses données à l'abri et faire la une des journaux réside souvent dans la capacité à rapidement identifier les tentatives d'exfiltration et à y remédier.

- **Visibilité sur les incidents de sécurité —** Par des vues personnalisées et des rapports, vous obtenez des aperçus synthétiques ou détaillés des incidents de sécurité et des mesures correctives correspondantes.
- **Mise en œuvre proactive de stratégies pour tous types d'informations —** La solution permet l'application de stratégies de protection, non seulement pour les informations sensibles connues mais aussi pour celles dont vous ignorez l'existence. Grâce à l'éventail étendu de stratégies intégrées, régissant notamment la conformité, l'utilisation acceptable ou encore la propriété intellectuelle, vous pouvez mettre en correspondance des documents entiers ou partiels avec un ensemble de règles, de façon à protéger la totalité de vos données sensibles.

McAfee DLP Endpoint

McAfee DLP Endpoint vous permet d'effectuer une surveillance instantanée et de prévenir l'exfiltration des données sur site, hors site et dans le cloud. En plus de surveiller rapidement les événements en temps réel, vous pouvez appliquer des stratégies de sécurité gérées de façon centralisée et générer des rapports détaillés en matière de prolifération et d'investigation numérique, le tout sans perturber les opérations habituelles.

- **Prise en charge améliorée de la virtualisation —** Les stratégies sont mises en œuvre en fonction de l'utilisateur et pour plusieurs sessions et infrastructures de postes de travail virtuels. Vous bénéficiez ainsi d'une flexibilité accrue et d'un meilleur contrôle sur les flux de données à destination des terminaux partagés.
- **Fonctions complètes de surveillance et de rapports sur les incidents —** La solution collecte toutes les données nécessaires à des fins d'analyse, d'investigation et d'audit, mais aussi d'évaluation des risques et de mesures correctives. Parmi les éléments de preuve rassemblés, citons entre autres l'expéditeur, le destinataire, l'horodatage et divers indices propres au réseau.
- **Console de gestion centralisée —** La solution tire parti de la console de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™) pour définir les stratégies, déployer et mettre à jour les agents, surveiller les événements en temps réel et générer les rapports permettant de répondre aux exigences de conformité.
- **Gestion complète du contenu —** La solution permet de contrôler et de bloquer la copie de données confidentielles sur des clés USB, des smartphones et autres périphériques de stockage amovibles, dont les disques optiques. L'intégration entre DLP et des solutions de gestion des droits numériques étend cette protection au-delà de votre réseau.

McAfee Device Control

McAfee Device Control empêche l'exfiltration de données via des supports et des unités de stockage amovibles tels que des clés USB, des CD et des DVD, ainsi que des smartphones. La solution permet à votre entreprise de surveiller et de contrôler les transferts de données à partir de tous les ordinateurs de bureau et ordinateurs portables, où qu'ils se trouvent, sur site ou hors site. McAfee Device Control offre de multiples fonctionnalités de blocage en fonction du contenu et du contexte :

- **Gestion complète des équipements et des données —** Vous pouvez contrôler la façon dont vos utilisateurs copient les données sur des clés USB, des smartphones, des CD et DVD enregistrables et de nombreux autres types de dispositifs pouvant être utilisés à des fins d'exfiltration de données.
- **Contrôles granulaires —** Device Control permet de spécifier les équipements dont l'utilisation est autorisée ou interdite, de définir les données dont la copie est admise ou interdite sur des équipements autorisés, et de bloquer la copie de données au départ d'emplacements et d'applications spécifiques.
- **Fonctionnalités avancées d'audit et de génération de rapports —** Le respect des exigences de conformité est simplifié grâce à une journalisation détaillée au niveau de l'utilisateur et de l'équipement. Des informations précises (équipement, horodatage, données concernées par l'événement, etc.) sont facilement consignées, présentées dans des rapports et peuvent ainsi servir d'éléments de preuve pour faciliter les enquêtes de conformité et d'audit.
- **Gestion centralisée —** L'intégration de la solution avec le logiciel McAfee ePO permet la surveillance des événements en temps réel et une gestion centralisée des stratégies et des incidents.

McAfee Next Generation Firewall

McAfee Next Generation Firewall vous protège contre l'exfiltration de données ou les attaques qui tirent parti des AET, ou techniques de contournement avancées. McAfee Next Generation Firewall effectue une inspection approfondie des paquets et procède à une normalisation du trafic de l'ensemble de la pile et à une inspection horizontale basée sur les flux de données. L'objectif est d'exposer les anomalies au sein du trafic, notamment la communication du logiciel malveillant avec son serveur de contrôle ou les tentatives d'exfiltration d'informations à partir du réseau.

- **Blocage des AET —** Utilise la normalisation du trafic multicouche, les empreintes basées sur les vulnérabilités et la comparaison des empreintes indépendantes des protocoles.
- **Détection des activités du serveur de contrôle —** Utilise la détection basée sur le déchiffrement et l'analyse de la séquence de longueur du message pour détecter les activités du réseau de robots et du serveur de contrôle.
- **Blocage basé sur la géolocalisation —** Interdit les connexions entrantes et sortantes en provenance et à destination des pays avec lesquels votre entreprise n'a pas de relations commerciales, afin de limiter le risque de recevoir des commandes du serveur de contrôle transmises par des adresses IP qui n'ont aucune raison de communiquer avec votre environnement.

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com